**Cybercriminals Don’t Care About Covid**

Covid may have stopped you from being able to go do your job, but these ransomware criminals still have their jobs. I found three things interesting in this article from “The Conversation”, by Nir Kshetri: What ransomware attacks are; what ransomware criminals want; and whether or not you should pay the required ransom.

**Ransomware Attacks**

Ransomware attacks are some of the deadliest cyber-attacks that are used in our world today. Ransomware is a malicious software that infects your computer and demands a fee be paid in order to get your system to work properly again. In an article from *The Conversation*, Nir Kshetri outlines how the ransomware criminals are now targeting large universities and their sensitive data. These criminals encrypt the colleges’ data and force them to pay a ransom in exchange for their data back safely. Kshetri states that “In 2019 alone, 89 U.S. universities, colleges, and school districts became victims of such attacks, followed by at least 30 in the first five months of 2020.” I believe that this will become even more of a problem as we become more and more reliant on technology to hold all of our sensitive information.

**Examples of Ransomware Attacks**

In an attack on June 1st, the University of California, San Francisco was breached by a criminal gang who targeted the medical school faculty’s research. These criminals used a malware called NetWalker. NetWalker targets corporate networks and encrypts the data that it finds on the attacked devices, denying the user access to the information until the ransom has been paid. Having a security system that is constantly being updated to the latest versions is crucial to stopping these kinds of attacks from happening in the first place. Another attack in March forced the Champaign-Urbana Public Health District to pay $350,000 in ransom money to retrieve 99% of their files back.

**Higher Education is the Target**

Kshetri says, “universities have become more attractive targets for cybercriminals because of their weak cybersecurity measures.” I could not agree more with his statement. These universities are not concerned about the safety of our information nearly as much as they should be. Mostly everything students do at school is through the universities’ wireless networks which gives these criminals easy access to all kinds of faculty, staff, and students’ information. There should be constant updates to the security system because of how quickly technology is advancing and changing. No university should be allowed to have weak, outdated security software because of how sensitive some of the data is that they are holding. I am sure that it won’t be difficult for them to find room in their budget to take on a professional to be In charge of keeping security systems up to date.

**Do you Pay the Ransom?**

Paying the ransom is always a tricky game to play in these types of scenarios. No one ever really knows if the criminals will hold up their end of the deal after they get what they want, which is why it can be a tough decision to make. Generally, law enforcement suggests opposing paying the ransom, while reporting it to the police as soon as possible, whether or not they are willing to make the ransom payments. KShetri states in the article that “in 2016, only ¼ of organizations that paid ransoms recovered their data.” This just goes to show that there is no guarantee that these criminals will hold up their side of the bargain. Some desperate victims may decide to pay and just hope that the criminals will hold up their end of the deal. To try and protect future losses, sometimes larger corporations and companies will buy cyber insurance. This will protect them from losses in the case they are ever attacked, which seems like one of the better solutions to protecting yourself from cybercriminals. So no one really has a correct answer for whether or not you should pay the ransom since these criminals are so unpredictable with their actions.

In conclusion, these cybercriminals are some of the deadliest of all criminals. Stealing others information and proceeding to make them pay to get their own information back is a power move. I hope that I was able to give a better understanding of what ransomware attacks are, and how you can deal with them if you are ever victim of one.